REMARKS

The Office Action mailed March 16, 2005 has been reviewed and carefully considered. The Examiner's reconsideration is respectfully requested in view of the above amendments and the following remarks.

Claims 1-10 are pending in the present application. Claims 1 and 8 have been amended. New claim 11 has been added. The amendments merely clarify the claims and no new issues are presented which would require further searching by the Examiner. No new matter has been added.

By the Office Action, claims 1, 2 and 8 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,636,968 to Rosner et al. (hereinafter Rosner) in view of U.S. Patent No. 5,604,801 to Dolan et al. (hereinafter Dolan).

Applicants respectfully traverse the rejections.

Rosner teaches a system and method for encrypting information for distribution to multiple recipients. However, Rosner's process is notably distinguishable from and fails to teach or suggest the present invention. Firstly, Applicants note the Examiner's assertion in the Office Action on page 2, stating that: "[T]he destination (subset) devices contain a first private key.." and: "[A] source (master) device (which is predetermined) communicates with the destination(subset) devices as shown in Figure 3." In accordance with this assertion and referring to FIGS. 2, 3 and 4 of Rosner, it is readily apparent that the alleged "master" device (source device 210) is distinct and separate from the alleged "subset" devices (destination devices 250, 260, 270, 280). Thus, Rosner clearly not only fails to disclose or suggest, but teaches away from, identifying a master device **from among** the subset of devices, as presently claimed in claims 1 and 8. That is, in Rosner, there is no 'master/slave' relationship within the asserted subset of devices, as taught and

claimed in the present invention. The present invention advantageously provides a secure sub-network in which any of the devices in the subset of devices may communicate with each other securely; Rosner simply focuses on an encryption/decryption system for key exchange between a predetermined source device and multiple destination devices.

Even assuming *arguendo*, that Rosner's source device 210 as well as the destination devices 250, 260, 270, 280 would have been asserted to comprise the presently claimed subset of devices, from which the source device 210 is alleged to be the "master" device, Rosner nevertheless fails to disclose or suggest the claimed step of identifying a master device from among the subset of devices that have scanned an access card, essentially as claimed in claims 1 and 8. Instead, in Rosner, the source device 210 is **predetermined**, as affirmed by the Examiner's statement in the Office Action at paragraph 2, lines 6-7. In contrast, the master device of the present invention is not predetermined, but rather is identified (determined) from among the subset of devices that have scanned an access card. While there is, in and of itself, a clear distinction between the step of determining something vs. something which has a predetermined designation, Applicant has amended claims 1 and 8 to replace "determining" with the term "identifying" as supported by the specification, e.g., on page 5, lines 32-34 to further emphasize this distinction.

Col. 3, lines 40-60 and Col. 4, lines 48-60, discussing session key 221 are cited in Rosner as teaching "a shared encryption key." However, careful review of Rosner reveals that a session key 221 is created that is based on a composite of the **public keys of each of the intended destination devices**, and a group key and partial keys are created that, when appropriately combined with a **corresponding** private key of the

intended destination device(s), provide a decryption key corresponding to the session key. *See* Col. 4, lines 17-24. That is, the session key 221 is based upon a secret key *x* of the source device and public keys 251a, 261a, 271a, 281a, etc. from each corresponding destination device. Thus, the source device 210 generates a **different** session key for each destination device; there is no "shared" encryption key between/amongst a subset of devices as in the present invention. In fact, a different session key for each destination device is critical in Rosner for effectuating selective encryption. The Abstract recites: "[I]ncluding or excluding the public key of selected destination devices in the creation of the session key effects selective encryption." And, Col. 5, lines 34-38 recites: "[N]ote that the session key K 221 is based upon the public key of each of the destination devices... This provides a method for selectively including or excluding one or more of the destination devices for authorized decryption." Rosner thus fails to disclose or suggest at least computing a shared encryption key, sending the shared encryption key to the subset of devices and requesting an encryption of any subsequent messages between any of the devices comprising the subset of devices using the shared encryption key, essentially as claimed in claims 1 and 8.

Unlike Rosner, in which selective encryption depends on exclusion/inclusion by a source device of particular public keys of destination devices, the present invention achieves selectivity in the devices to be included in a secure sub-network for secure communication namely via the provision and scanning of an access card for scanning by the included devices. Advantageously, an access card according to the present invention provides an independent means for quickly designating devices to be included in a secure sub-network without requiring, e.g., updating a source device with newly added

destination devices. Rosner fails to disclose or suggest at least the steps of providing an access card having a first private key, and scanning the access card to determine the first private key, by the subset of devices, essentially as claimed in claims 1 and 8 and as affirmed by the Examiner on page 2 of the Office Action.

Applicants have carefully reviewed Dolan but find it fails to cure the deficiencies of Rosner. Dolan is cited as generally disclosing "...a card containing a private key which is used for encrypted communications." However, Applicants review of Dolan reveals disclosure of a server 130 for performing public key processing using a private key unique to one or more users. The server 130 stores/has access to the private key in encrypted form only (being encrypted with a key encrypting key). A security device 120 includes means for storing or generating the key encrypting key and providing the key encrypting key to the server. *See* Abstract. That is, the security device controls the public key processing by providing **the server** with a key to enable the server to decrypt the private key, use it, and delete the private key after use. *See* Col. 3, lines 22-27.

However, Dolan clearly fails to disclose or suggest at least **scanning an access card** to determine the first private key **by each of a subset of devices**, essentially as claimed in claims 1 and 8. Instead, in Dolan, the security device merely provides a key to **the server** 130, which in turn processes the message for an intended recipient 140. Even assuming, *arguendo,* that its security device 120 was equivalent to the access card of the present invention, Dolan lacks any teaching or disclosure for providing its alleged 'private key' on a 'smart card' to each device of a secure sub-network for secure communication therein, as in the present invention.

Accordingly, claims 1 and 8 are believed to be allowable over Rosner in view of Dolan. Claim 2 depends directly on claim 1. As such, the Applicants respectfully submit that the dependent claim is patentable and nonobvious for at least the reasons given above for claim 1.

Claims 3-7, 9 and 10 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,636,968 to Rosner et al. (hereinafter Rosner) in view of U.S. Patent No. 5,604,801 to Dolan et al. (hereinafter Dolan) and further in view of U.S. Patent No. 6,490,680 to Scheidt et al. (hereinafter Scheidt).

The rejection of claims 3-7, 9 and 10 is based, in part, on the Examiner's contention that Rosner in view of Dolan disclose or suggest the features of claims 1 and 8, from which such claims respectively depend. Without addressing the specific rejections, however, it is clear that the combination of Rosner, Dolan and and Scheidt is legally deficient since, at the very least, as explained above, neither Rosner and/or Dolan disclose or suggest the features of claims 1 and 8, from which claims 3-7 and 9-10 respectively depend.

Accordingly, claims 3-7 and 9-10 are believed to be patentable and nonobvious over Rosner in view of Dolan and Scheidt for at least the reasons given above for claims 1 and 8.

Accordingly, the Applicants respectfully request withdrawal of all the rejections under 35 U.S.C. §103(a), and allowance of pending claims 1-11 on the merits.

In view of the foregoing amendments and remarks, it is respectfully submitted that all the claims now pending in the application are in condition for allowance.

CONCLUSION

In view of the foregoing amendments and remarks, it is respectfully submitted that claims 1-11 are patentable and nonobvious over the cited references. Consequently, the Applicants respectfully request reconsideration and withdrawal of the rejections and allowance of the application. Such early and favorable action is earnestly solicited.

No fees are believed to be due at this time. The office is hereby authorized to charge any additional fees which may be required in connection with this amendment and to credit any overpayment to our Deposit Account No. 07-0832.

Respectfully submitted,

Dated: 14 June 2005

By: _____
Joseph Kolodka
Registration No. 39,731

CORRESPONDENCE ADDRESS:

THOMSON LICENSING INC.
2 INDEPENDENCE WAY
P.O. BOX 5312
PRINCETON, NJ 08540